Review Seminararbeit

Seminar Software Engineering für verteilte Systeme

Daniel Sturm (1453079)

SoSe 2024

Hinweise

- Länge des Reviews: 2–3 Seiten (inklusive dieser Hinweise)
- Jede Frage in diesem Template muss beantwortet werden! **Ersetzen** Sie dazu die vorhandenen `\todo`-Befehle im Template durch Ihre Antworten in Fließtext oder ausführlichen Stichpunkten.
- Die Qualität der von Ihnen verfassten Reviews geht in Ihre Gesamtnote für das Seminar ein.
- Entfernen Sie nach dem vollständigen Bearbeiten des Reviews das `todonotes`-Paket im Header dieser Datei. Wenn Sie alle `\todo`-Befehle ersetzt haben, kompiliert das Dokument weiterhin ohne Fehler. `\usepackage[color=smdsblue!25]todonotes`

Allgemeine Informationen

Titel der zu bewertenden Arbeit

Grafana: Sicherheitsaspekte in verteilten Systemen - Herausforderungen und Maßnahmen

Hauptinhalt der Arbeit

Zu Beginn der Arbeit wird ein Überblick über Grafana gegeben. Hierbei wird das Open-Source-Tool zur Visualisierung und Überwachung von IT-Systemen vorgestellt. Besonders hervorgehoben werden dabei die Integration von verteilten Datenquellen über diverse Datenbanken sowie die Möglichkeit zur Erstellung von Alerts. Zum Ende der Einleitung wird die Zielsetzung der Arbeit mit der Frage nach den Sicherheitsaspekten von Grafana in verteilten Systemen formuliert.

Im zweiten Kapitel werden die benötigten Grundlagen über Cyber Security und verteilte Systeme beschrieben. Hierzu wird zuerst auf das CIA-Triad sowie auf die ISO/IEC 27001 als Basis für Informationssicherheit eingegangen. Anschließend wird die Relevanz von Cyber Security insbesondere für Grafana, als ein verteiltes System mit Zugriff auf viele Datenquellen, erläutert.

Im weiteren Verlauf der Arbeit werden die Sicherheitsfunktionen von Grafana erläutert. Hierbei wird zuerst auf das Identity and Access Management (IAM) eingegangen. Ein wichtiger Bestandteil hierbei ist der Schutz der Datenquellen sowie der Dashboards. Die Verschlüsselung von Datenbanken sowie das Auditing stellen weitere wichtige Sicherheitsfunktionen dar. Außerdem bietet Grafana die Möglichkeit zum Blacklisting zur Verhinderung von DDoS-Angriffen sowie die Möglichkeit des Abgleichs von möglicherweise geleakten Service-Tokens. Allgemeine Sicherheitsmaßnahmen wie das

regelmäßige Updaten von Grafana, Backups und verschlüsselte Kommunikation spielen selbstverständlich auch eine wichtige Rolle.

Zur Evaluation der Sicherheitsaspekte von Grafana wird die Open-Source-Version mit der Cloud-/Enterprise-Version verglichen. Essenziell ist hierbei, dass gerade bei der Nutzung durch viele Benutzer essentielle Sicherheitsfunktionen wie Berechtigungen für Datenquellen, Key Management Service, Audit Logging und automatische Updates nur in der kostenpflichtigen Version verfügbar sind.

Allgemeine Bewertung

Stärken der Arbeit

- Gute Einleitung in das Thema Grafana und enges Arbeiten an der Grafana-Dokumentation.
- Gut beschrieben, warum die Sicherheit von Grafana wichtig ist (viele Datenquellen, DDoS, Single Point of Failure).
- Klar gegliederter Aufbau der Maßnahmen und Herausforderungen.

Schwächen der Arbeit

- Schon in der Einleitung das Ziel der Evaluation zwischen kostenloser und kostenpflichtiger Version beschreiben.
- Ist die Enterprise-Version dann sicher oder hat sie auch noch Schwächen?
- Penetrationstests oder Ansätze zur Umgehung von Sicherheitsmaßnahmen wären interessant.
- Genauer auf sichere Kommunikation eingehen (Protokolle wie HTTPS genauer erläutern, wie erfolgt der Zugriff auf die Daten, eventuell Fallbeispiel von verteilten Systemen einbeziehen).

Nutzung KI-basierter Tools

Denke es kam kein KI-basiertes Tools höchstens zur Rechtschreibprüfung und Grammatikprüfung zum Einsatz, was sich aber nicht nachweisen lässt.

Sachliche Korrektheit

Die Sachliche Korrektheit ist gegeben. Es wird im wesentlichen auf Grafana Labs (die offzielle Dokumentation) verwiesen. Der Nutzerbericht ist in der Arbeit klar als solcher gekennzeichnet.

Äußere Form

- Präzise Wortwahl: „Auditing in Grafana bezieht sich auf den Prozess der Überwachung und Aufzeichnung von Aktivitäten, die in Grafana stattfinden.“ (Seite 4)
- Korrekte Verwendung von Fachterminologie: „Grafana bietet verschiedene Authentifizierungsmethoden, um einen sicheren Zugriff auf die Plattform zu gewährleisten. Dazu gehören die Authentifizierung über Benutzername und Passwort, SAML, OAuth und mehr.“ (Seite 3)

- Korrekte Kommasetzung: „Ein weiteres wesentliches Element der Sicherheit ist die Datenbankverschlüsselung, wobei das regelmäßige Rotieren der Schlüssel meist ausreichend ist.“ (Seite 6)
- Einteilung und roter Faden sind ersichtlich und gut strukturiert: Vorstellung => Relevanz => Herausforderungen => Maßnahmen => Evaluation => Schluss
- Angemessene Verwendung von Abbildungen: Abbildung 1 (Grafana-Beispiel) ist gut für die Vorstellung; Tabelle 1 ist sinnvoll für die Evaluation
- Abbildungen und Tabellen sind gut beschriftet
- Abbildungen und Tabellen werden im Fließtext referenziert
- Das Erscheinungsbild ist gut